

802.11n Modular WLAN Access Point

User Guide

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Table of Contents

1. Introduction	1
1.1. Overview.....	1
1.2. Features.....	1
1.3. LED Definitions	3
2. First-Time Installation and Configuration	4
2.1. Power.....	4
2.2. Installing the Access Point.....	4
2.3. Connecting a Managing Computer.....	5
2.4. Configuring the AP	6
2.4.1. Login.....	6
2.4.2. Selecting Mode	7
2.4.3. Configuring TCP/IP Settings.....	8
2.4.4. Configure IEEE 802.11 Settings.....	9
2.4.5. Review and Apply Settings.....	10
2.5. Setting up Client Computers	11
2.5.1. Configure IEEE 802.11 Settings.....	11
2.5.2. Configure TCP/IP-Related Settings	11
2.6. Confirm Settings of the Access Point and Client Computers.....	12
2.6.1. Checking if the IEEE 802.11n-Related Settings Work.....	12
2.6.2. Checking if the TCP/IP-Related Settings Work	12
3. Advanced Network Management.....	12
3.1. Overview.....	13
3.1.1. Menu Structure	13
3.1.2. Save, Save & Restart, and Cancel Commands.....	14
3.1.3. Home and Refresh Commands	15
3.2. Viewing Status	15
3.2.1. Associated Wireless Clients	15
3.2.2. Current DHCP Mappings.....	16
3.2.3. System Log.....	16
3.2.4. Link Monitor	17
3.3. General Operations	17
3.3.1. Specifying Operational Mode	17
3.3.2. Changing Password	18
3.3.3. Managing Firmware	19
3.3.3.1. Upgrading Firmware by HTTP.....	19
3.3.3.2. Backing up and Restoring Configuration Settings by HTTP	19
3.3.3.3. Upgrading Firmware by TFTP	20
3.3.3.4. Backing up and Restoring Configuration Settings by TFTP	22
3.3.3.5. Resetting Configuration to Factory Defaults.....	23
3.4. Configuring TCP/IP Related Settings	23
3.4.1. Addressing.....	23
3.4.2. DHCP Server.....	24
3.4.2.1. Basic.....	24
3.4.2.2. Static DHCP Mappings.....	24
3.5. Configuring IEEE 802.11 Related Settings	25
3.5.1. Communication.....	25
3.5.1.1. Basic.....	25
3.5.1.2. Link Integrity	26
3.5.1.3. Association Control	26
3.5.1.4. Load Balancing.....	26
3.5.1.5. Wireless Distribution System.....	26
3.5.2. Security.....	29
3.5.2.1. Selecting Wireless Security Mode	30

3.5.2.2. MAC-Address-Based Access Control	31
3.5.3. IEEE 802.1x/RADIUS	33
3.6. Advanced Settings	35
3.6.1. Packet Filters	35
3.6.1.1. Ethernet Type Filters	35
3.6.1.2. IP Protocol Filters	35
3.6.1.3. TCP/UDP Port Filters	36
3.6.2. Management	36
3.6.2.1. UPnP	36
3.6.2.2. System Log	37
3.6.2.3. SNMP	37
Appendix A: Default Settings	39
Appendix B: Troubleshooting	40
B-1: Wireless Settings Problems	40
B-2: TCP/IP Settings Problems	41

1. Introduction

1.1. Overview

The Access Point modular WLAN access point (AP) enables 802.11n or 802.11g client computers to access the resources on an Ethernet network wirelessly or wired. It conveniently fits into standard wall outlets and only takes a few minutes to install and configure for use. The Access Point has a built-in browser-based management application offering an easy to follow setup-wizard for novice wireless users as well as comprehensive settings for more advanced users and/or network administrators.

1.2. Features

- **Access Point Firmware Features**

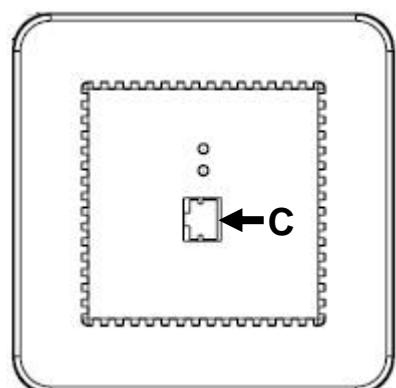
- **Operational Modes**
 - ◆ **AP/Bridge.** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
 - ◆ **AP Client.** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendor.
- **RF Type Selection.** The RF type of the WLAN interface can be configured to work in IEEE 802.11n only, IEEE 802.11g only, IEEE 802.11g only, or mixed mode (802.11n, 802.11g and 802.11b simultaneously).
- **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For authentication and data encryption.
- **Enabling/Disabling SSID Broadcasts.** When the Access Point is in AP/Bridge mode, the administrator can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcast functionality is disabled, a client computer cannot connect to the Access Point with “blank” network name (SSID, Service Set ID); the correct SSID has to be specified on client computers.
- **MAC-address-based Access Control.** When the Access Point is in AP/Bridge mode, it can be configured to block unauthorized wireless client computers based on MAC (Media Access Control) addresses. Additionally, an ACL (Access Control List) can be downloaded from a TFTP server.
- **IEEE 802.1x/RADIUS.** When the Access Point is in AP/Bridge mode, it can be configured to authenticate wireless users and distribute encryption keys dynamically by IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service).
- **WPA (Wi-Fi Protected Access).** The Access Point supports the WPA standard proposed by the Wi-Fi Alliance (<http://www.wi-fi.org>). Both WPA-PSK (Pre-Shared Key) mode and full WPA mode are supported. WPA is composed of TKIP (Temporal Key Integrity Protocol) and IEEE 802.1x and serves as a successor to WEP for better WLAN security.

- **Repeater.** When the Access Point is in AP/Bridge mode, it can communicate with other APs or wireless bridges via WDS (Wireless Distribution System). Therefore, a Access Point can wirelessly forward packets from wireless clients to another Access Point. Then the second Access Point forwards the packets to the Ethernet network.
- **Wireless Client Isolation.** When the Access Point is in AP/Bridge mode, wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users' computers.
- **AP Load Balancing.** Several Access Point's can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the devices. This function is available when the Access Point is in AP/Bridge mode.
- **Transmit Power Control.** Transmit power of the Access Point's RF module can be adjusted to desired RF coverage.
- **Link Integrity.** When the Access Point is in AP/Bridge mode and its Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the Access Point and no wireless client can associate with it.
- **Association Control.** When the Access Point is in AP/Bridge mode, it can be configured to deny association requests when it has served too many wireless clients or traffic load is too heavy.
- **Associated Wireless Clients Status.** When the Access Point is in AP/Bridge mode, it can show the status of all wireless clients that are currently associated or 'connected'.
- **Auto Channel Selection.** The auto channel selection feature allows the device to automatically select the channel that will provide optimum performance on powering up the Access Point.
- **DHCP client.** The Access Point can automatically obtain an IP address from a DHCP server.
- **DHCP server.** The Access Point can automatically assign IP addresses to computers or other devices by DHCP (Dynamic Host Configuration Protocol).
- **Static DHCP Mappings.** The administrator can specify static IP address to MAC address mappings so that IP addresses are always assigned to the hosts with the specified MAC addresses.
- **Showing Current DHCP Mappings.** Displays which IP address is assigned to which host identified by an MAC address.
- **Packet Filtering.** The Access Point provides Layer 2, Layer 3, and Layer 4 filtering capabilities.
- **Firmware Management Tools**
 - **Firmware Upgrade.** The firmware of the Access Point can be upgraded in the following methods:
 - ◆ **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).

- ◆ **HTTP-based.** Upgrading firmware by HTTP (HyperText Transfer Protocol).
- **Configuration Backup.** The configuration settings of the Access Point can be backed up to a file via [TFTP](#) or [HTTP](#) for later restoring.
- **Configuration Reset.** Clears current configuration settings and restores to factory-default values.
- **Management**
 - **Browser-based Network Manager** for configuring and monitoring the Access Point via a Web browser. The management protocol is HTTP (Hyper Text Transfer Protocol)-based.
 - **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, and Private Enterprise MIB are supported.
 - **UPnP.** The Access Point responds to UPnP discovery messages so that a Windows XP user can locate the Access Point in My Network Places and use a Web browser to configure it.
 - **System Log.** For system operational status monitoring.
 - ◆ **Local log.** System events are logged to the on-board RAM of the Access Point and can be viewed using a Web browser.
 - ◆ **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.
- **Power over Ethernet.** Power is supplied to the Access Point via an Ethernet cable using an 802.3af compliant power injector.
- **Hardware Watchdog Timer.** If the firmware “hangs” in an invalid state, the hardware watchdog timer will detect this situation and restart the Access Point. This way, the Access Point can provide continuous services.

1.3. LED Definitions

There are several LED indicators on the front of the Access Point. Please refer to the definitions below:



- A. **WAN**: Green, solid when connected, flashing when data activity
- B. **Wireless**: Green, solid when on, flashing when wireless data activity
- C. **RJ-45 LAN port**
 - Amber, solid when LAN connection
 - Green, solid when LAN connection, flashing when activity

2. First-Time Installation and Configuration

2.1. Power

The Access Point is powered using PoE (Power over Ethernet). The Access Point automatically selects the suitable power supply.

To power the AP by PoE:

1. Plug one connector of an Ethernet cable to an available port of a PoE injector or switch.
2. Plug the other connector of the Ethernet cable to the **WAN** port on the rear of the Access Point.

NOTE: The Access Point is 802.3af compatible.

2.2. Installing the Access Point

The Access Point has two options for installation: desktop/flat surface or into a standard Ethernet wall jack.

Desktop or flat surface:

1. Remove the Access Point from the box and snap apart the two pieces of the screw less faceplate that are affixed to the Access Point.
2. Place the Access Point in desired location upon the desk or flat surface.
3. Using the single-port PoE Injector, connect one end of an Ethernet LAN cable from a LAN port on the network router or switch and the opposite end to the port marked “Data In”. Use another Ethernet LAN cable to connect the port marked “Data Out” to the WAN port (on rear) of the Access Point.
4. Plug the single-port PoE power cord into an electrical outlet.
5. Check the LED indication lights. Two LEDs (WAN, Wireless) should be properly lit.

Ethernet Wall Jack:

1. Remove the Ethernet wall jack faceplate.
2. Plug the wall jack LAN cable to the WAN port, the rear port, of the main housing of Access Point. All two green LEDs on the Access Point should be lit if properly connected to a router/switch and PoE power supply. If “yes”, proceed to step 3.
3. Slowly insert the Access Point into the wall box until the main housing of Access Point is flush to

the wall.

4. Fasten the Access Point main housing to the wall box with screws provided.
5. Line-up and push the faceplate cover onto the main housing until it snaps securely into place.

2.3. Connecting a Managing Computer

To configure the Access Point using the **Advanced** option, a *managing computer* with a Web browser is needed.

NOTE: If you are using the browser, *Opera*, to configure the Access Point, click the menu item **File**, click **Preferences...**, click **File types**, and edit the MIME type, **text/html**, to add a file extension “.sht” so that Opera can work properly with the Web management pages of the AP.

Since the configuration/management protocol is HTTP-based, make sure that **the IP address of the managing computer and the IP address of the managed AP are in the same IP subnet** (the default IP address of the Access Point is **Obtain from DHCP Server**).

NOTE: When the AP failed to obtain IP from DHCP Server, after 3 attempts, the AP will set the default IP to 192.168.100.1.

To connect the Ethernet managing computer and the managed Access Point for first-time configuration, you have two choices as illustrated in Fig. 1.

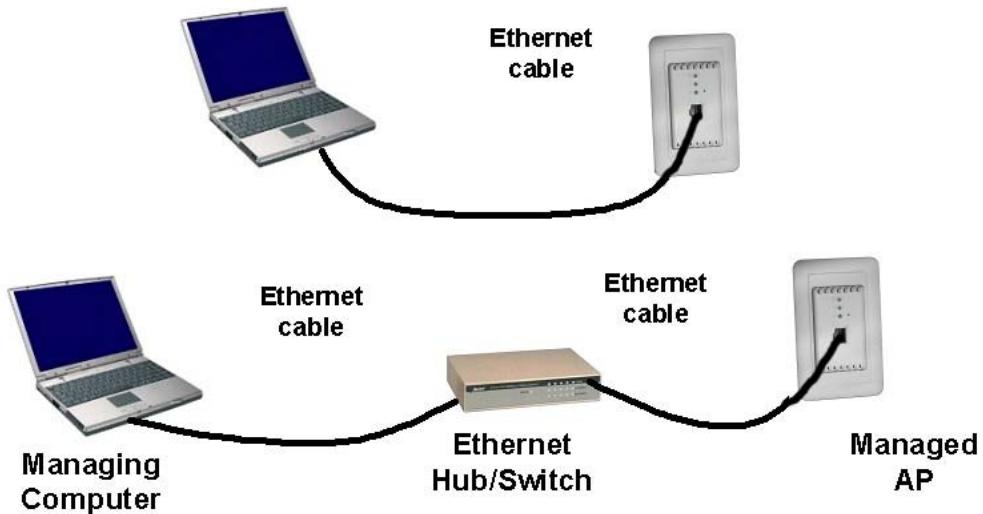


Fig. 1. Connecting a managing computer and the Access Point via Ethernet

You can use either a standard Ethernet cable (included in the package) or a switch/hub with two normal Ethernet cables.

NOTE: One connector of the Ethernet cable must be plugged into the Access Point WAN port for configuration.

2.4. Configuring the AP

After the IP addressing issue is resolved, launch a Web browser on the managing computer. Then, go to “<http://AP IP>” to access the *Web-based Network Manager* login page.

TIP: The Access Point can be reached by its *host name* using a Web browser. For example, if the Access Point is named “AP”, you can use the URL “<http://AP>” to access.

2.4.1. Login

Before the Home page is shown, you will be prompted to enter the user name and password to gain the right to access the Web-based Network Manager. For first-time configuration, use the default user name “**admin**” and default password “**admin**”, respectively.

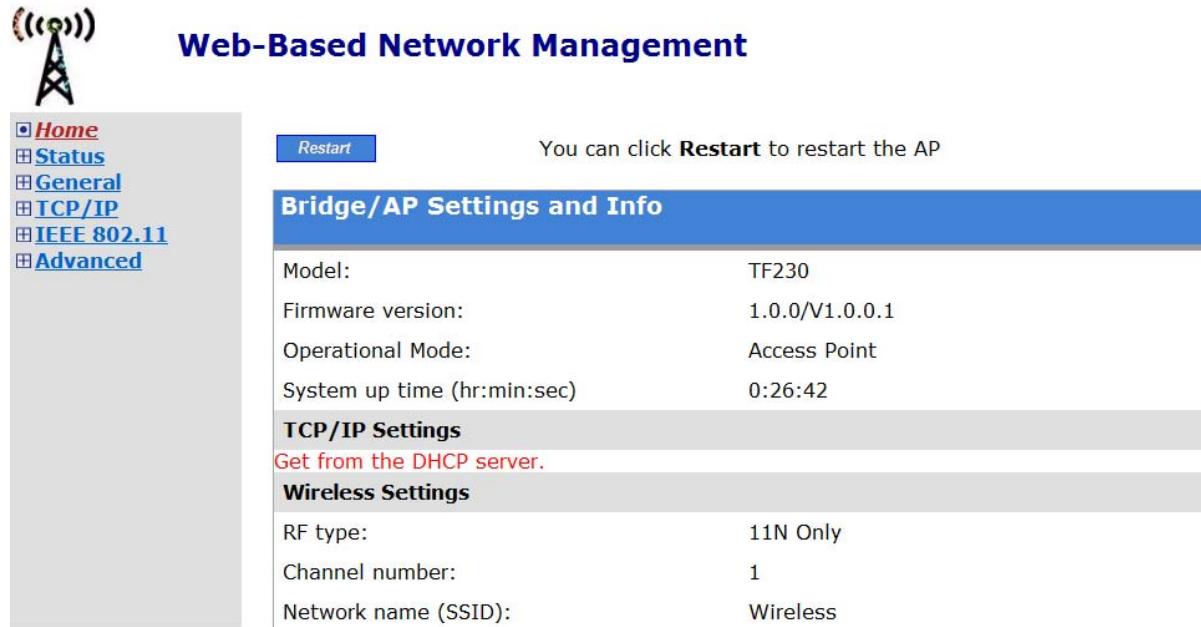


The screenshot shows the login interface for the Web-Based Network Management system. At the top left is a logo of a tower with signal bars. To its right, the text "Web-Based Network Management" is displayed in a bold, blue, sans-serif font. Below the logo and text, a message reads "Please type your user name and password." A horizontal line with a break in the middle separates this message from the input fields. The first field is labeled "User name:" and contains a single character "A". The second field is labeled "Password:" and is empty. At the bottom left of the form is a blue "Log On" button with white text.

Fig. 2. The Login page

NOTE: It is strongly recommended that the password be changed for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 3.3.1 for more information).

Once you have successfully logged in, the Home page opens. Click on the main manual on left hand side for **Setup**.



Web-Based Network Management

Bridge/AP Settings and Info

Model:	TF230
Firmware version:	1.0.0/V1.0.0.1
Operational Mode:	Access Point
System up time (hr:min:sec)	0:26:42

TCP/IP Settings
Get from the DHCP server.

Wireless Settings

RF type:	11N Only
Channel number:	1
Network name (SSID):	Wireless

Fig. 3. The Home page

2.4.2. Selecting Mode

The Access Point supports two operational modes:

- **AP/Bridge.** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- **AP Client.** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

<input checked="" type="radio"/> AP / Bridge This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
<input type="radio"/> AP Client This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Fig. 4. Operational mode settings

1. Click on **General** from the side menu, and then select **Operational Mode**.
2. Select an operational mode and click **Save** to apply the setting.

In either mode, the Access Point forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are two types of wireless links as specified by the IEEE 802.11 standard.

- **STA-AP.** This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The AP Client mode is actually an STA.
- **WDS.** This type of wireless link is established between two IEEE 802.11 Access Point's. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP/Bridge	AP Client
AP/Bridge	WDS	STA-AP
AP Client	STA-AP	

Table 1. Operational modes vs. wireless link types.

To establish a *static* bridge link based on WDS, the AP/bridges at both end of the WDS link must be *manually* configured with each other's MAC addresses (see Section 3.5.1.5 for more information). To establish a *dynamic* bridge link between an Access Point and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any Access Point that is using the matched SSID and establishes a bridge link with the scanned Access Point.

NOTE: Although it's more convenient to use dynamic bridging, it has a limitation—the AP Client only can forward TCP/IP packets between its wireless interface and Ethernet interface; other type of traffic (such as IPX and AppleTalk) is not forwarded.

TIP: When the Access Point is configured to be in AP Client, it can be used as an Ethernet-to-wireless network adapter. For example, a notebook computer equipped with an Ethernet adapter can be connected to this device with a crossover Ethernet cable for wireless connectivity to another access point.

2.4.3. Configuring TCP/IP Settings

The IP address can be manually set or automatically assigned by a DHCP server on the LAN. If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the AP.



Web-Based Network Management

Home
Status
General
TCP/IP
 • Addressing
 • DHCP Server
IEEE 802.11
Advanced

TCP/IP Addressing

Method of obtaining an IP address: Obtain from a DHCP Server

IP address: 192.168.100.1

Subnet mask: 255.255.255.0

Default gateway: 192.168.100.254

Host name: 11n AP

Domain (DNS suffix):

Save Save and Restart Cancel

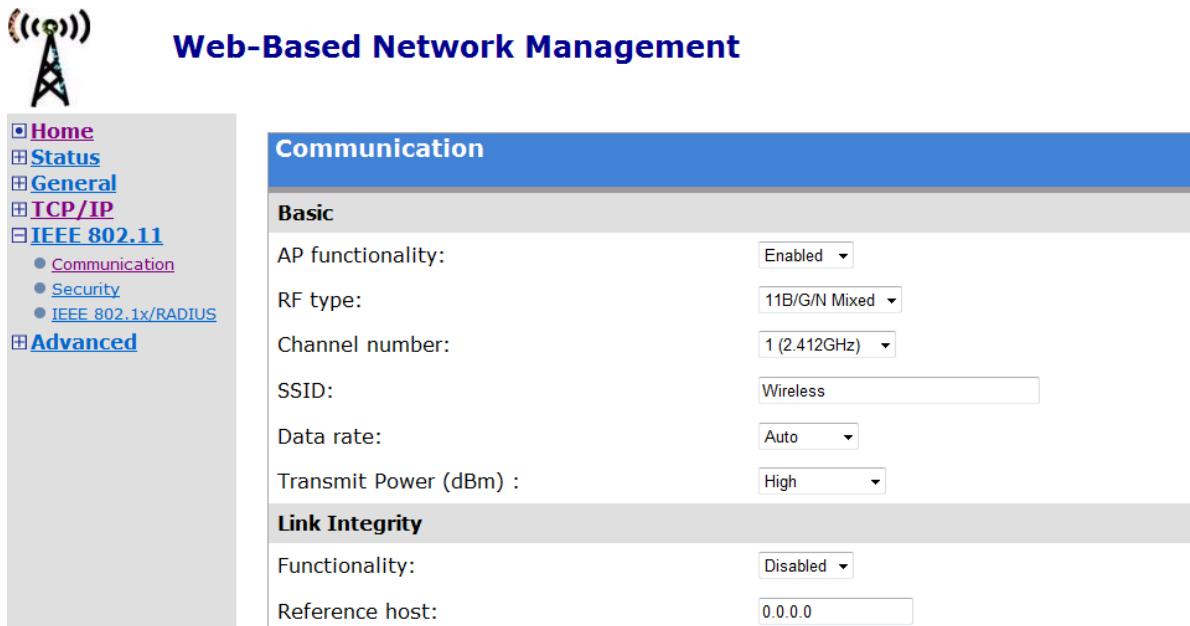
Fig. 5. TCP/IP settings.

1. Click on **TCP/IP** from the side menu and select **Addressing**.
2. When you have finished making changes, click **Save** or **Save & Restart**.

2.4.4. Configure IEEE 802.11 Settings

The Network Manager utility allows the user to configure IEEE 802.11n-related communication settings, including **Regulatory domain**, **Channel number**, and **Network name (SSID)** of the Access Point. The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. **The SSID of a wireless client computer and the SSID of the Access Point must be identical for them to communicate with each other.**

NOTE: Put a check in the **Auto Channel Selection** checkbox to allow the **Frequency Channel** of the Access Point to be automatically set.



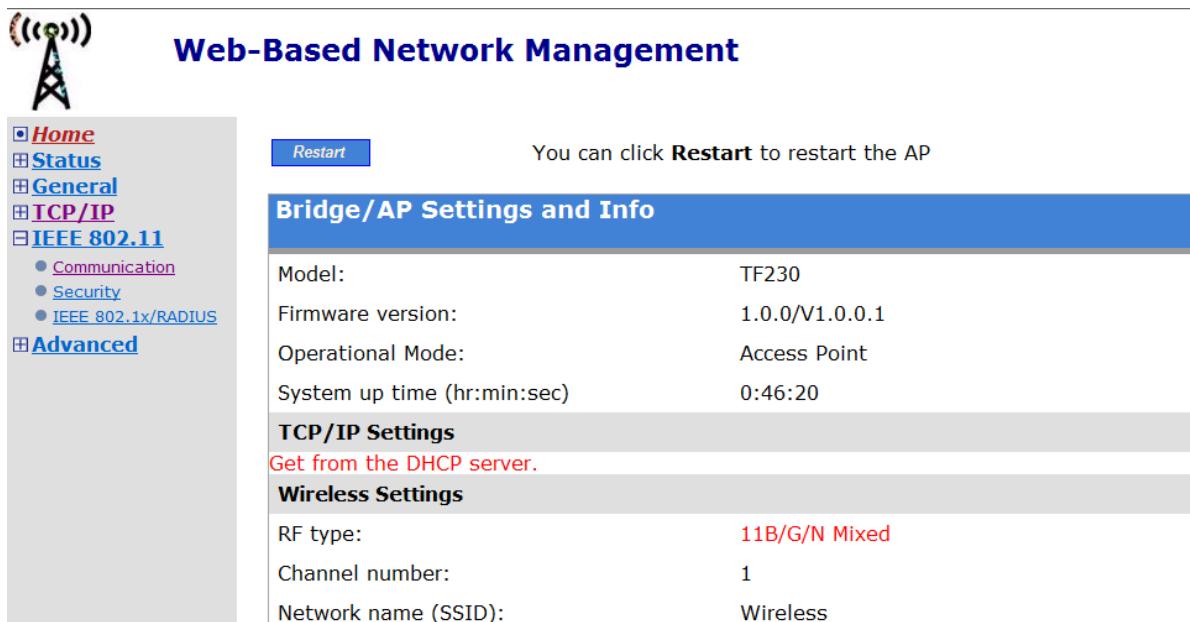
The screenshot shows the 'Communication' settings for IEEE 802.11. The 'Basic' section includes fields for AP functionality (Enabled), RF type (11B/G/N Mixed), Channel number (1 (2.412GHz)), SSID (Wireless), Data rate (Auto), and Transmit Power (dBm) (High). The 'Link Integrity' section includes fields for Functionality (Disabled) and Reference host (0.0.0.0). The sidebar on the left lists 'Home', 'Status', 'General', 'TCP/IP', 'IEEE 802.11' (with 'Communication' selected), and 'Advanced'.

Fig. 6. IEEE 802.11n communication settings

1. Click on **IEEE 802.11** from the side menu, and then select **Communication**.
2. When you have finished, scroll to the bottom of the screen and click either **Save** or **Save & Restart**.

2.4.5. Review and Apply Settings

On the Summary page, you can review all the settings you have made. Changes are highlighted in red. If they are OK, click **Restart** to restart the Access Point for the new settings to take effect.



The screenshot shows the 'Bridge/AP Settings and Info' section. It includes fields for Model (TF230), Firmware version (1.0.0/V1.0.0.1), Operational Mode (Access Point), and System up time (hr:min:sec) (0:46:20). Below this is a 'TCP/IP Settings' section with a note 'Get from the DHCP server.' and a 'Wireless Settings' section. The 'Wireless Settings' section shows RF type (11B/G/N Mixed), Channel number (1), and Network name (SSID) (Wireless). The sidebar on the left lists 'Home', 'Status', 'General', 'TCP/IP', 'IEEE 802.11' (with 'Communication' selected), and 'Advanced'. A 'Restart' button is visible on the left, and a note 'You can click **Restart** to restart the AP' is displayed above the settings table.

Fig. 7. Settings changes are highlighted in red.

TIP: Since the Home page shows the current settings and status of the AP, it can be saved or printed within the Web browser for future reference.

NOTE: Allow 7 seconds for the Access Point to complete its restart process.

2.5. Setting up Client Computers

The TCP/IP and IEEE 802.11n-related settings of wireless client computers must match those of the Access Point in order for a wireless link to be established.

2.5.1. Configure IEEE 802.11 Settings

Before the TCP/IP networking system of a wireless client computer can communicate with other hosts, the underlying wireless link must be established between a wireless-enabled computer and the Access Point.

To establish a wireless link:

Launch the configuration/monitoring utility provided by the vendor of the installed wireless adapter

OR

Use the automatic wireless network connection feature in Windows XP.

NOTE: A wireless client computer must be in *infrastructure* mode, so that it can associate with an AP.

NOTE: The SSID of the wireless client computer and the SSID of the Access Point must be identical. Or, in case the **SSID broadcasts** capability of the Access Point is enabled (by default), the SSID of the wireless client computer could be set to “any”.

NOTE: Both the wireless client computer and the Access Point must have the same WEP settings for them to communicate with each other.

NOTE: For better wireless security, IEEE 802.1x capability of the Access Point must be enabled so that only authenticated wireless users can access the wireless network.

2.5.2. Configure TCP/IP-Related Settings

Use **Windows Network Control Panel Applet** to change the TCP/IP settings of the client computers, so that the IP addresses of the client computers and the IP address of the Access Point are in the same IP subnet.

If a client computer is originally set a static IP address, you can either change its IP address to match the IP address of the AP, or select an automatically-obtain-an-IP-address option if there is a DHCP server on the network.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

2.6. Confirm Settings of the Access Point and Client Computers

After configuring the Access Point and setting up client computers, it is recommended that all settings are checked and confirmed.

2.6.1. Checking if the IEEE 802.11n-Related Settings Work

To check if a wireless client computer can associate with the AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.
2. Check if the client computer is associated to an access point, and the access point is the Access Point.

If the check fails, see Appendix B-1, “Wireless Settings Problems” for troubleshooting.

2.6.2. Checking if the TCP/IP-Related Settings Work

To check if a client computer can access the Internet:

1. Open a **Windows Command Prompt** window on the client computer.
2. Type “**ping *advap***”, where *advap* is a placeholder for the IP address of the AP. Replace it with your real IP address—for example, 192.168.0.1. Then press **Enter**.

If the Access Point responds, go to the next step; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

3. Type “**ping *default_gateway***”, where *default_gateway* is a placeholder for the IP address of the default gateway of the wireless client computer. Then press **Enter**.

If the gateway responds, go to the next step; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

4. Type “**ping *1st_dns_server***”, where *1st_dns_server* is a placeholder for the IP address of the primary DNS server of the wireless client computer. Then press **Enter**.

If this DNS server responds, go to the next step; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

5. Type “**ping *2nd_dns_server***”, where *2nd_dns_server* is a placeholder for the IP address of the secondary DNS server of the wireless client computer. Then press **Enter**.

If this DNS server responds the client should have no problem with TCP/IP networking; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

3. Advanced Network Management

This section covers the options and settings available in the ‘Advanced’ mode of the Web-based Network Manager utility.

3.1. Overview

To enter, simply click on the “Advanced” option on the Home page after login.

The screenshot shows the 'Web-Based Network Management' interface. On the left, a sidebar menu includes Home, Status, General, TCP/IP, IEEE 802.11, and Advanced (which is selected, showing sub-options for Packet Filter and Management). The main content area has a 'Restart' button and a note: 'You can click **Restart** to restart the AP'. Below this is a 'Bridge/AP Settings and Info' section with the following data:

Model:	TF230
Firmware version:	1.0.0/V1.0.0.1
Operational Mode:	Access Point
System up time (hr:min:sec)	0:46:20

Below this is a 'TCP/IP Settings' section with the note 'Get from the DHCP server.' and a 'Wireless Settings' section with the following data:

RF type:	11B/G/N Mixed
Channel number:	1
Network name (SSID):	Wireless

Fig. 8. The Summary page

3.1.1. Menu Structure

The left side of the screen contains a menu for you to carry out commands. Here is a brief description of the menu options:

- **Home.** Click this tab to return to the Home page.
- **Summary.** Click this tab to view a screen with at-a-glance status information.
- **Status.** Click this tab to access the following settings:
 - **Wireless Clients.** The status of the wireless clients currently associated with the AP.
 - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.
 - **System Log.** System events log.
 - **Link Monitor.** When the Access Point is in *AP Client* mode, this page shows the signal strength and link quality of the wireless link to its associated access point.
- **General.** Click this tab to access the following settings:
 - **Operational Mode.** Operational mode of the Access Point —*AP/Bridge* or *AP Client*.
 - **Password.** Modify the login settings.
 - **Firmware Tools.** For upgrading the firmware of the Access Point, backing up and restoring configuration, and configuration reset settings of the Access Point.

- **TCP/IP.** Click this tab to access the following settings:
 - **Addressing.** Modify IP address settings of the Access Point.
 - **DHCP Server.** Modify settings for the DHCP (Dynamic Host Configuration Protocol) server.
- **IEEE 802.11.** Click this tab to access the following settings:
 - **Communication.** Modify basic IEEE 802.11n/b/g settings of the Access Point to work properly with wireless clients.
 - **Security.** Modify security settings for authenticating wireless users and encrypting wireless data.
 - **IEEE 802.1x/RADIUS.** Modify IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service) security settings.
- **Advanced.** Advanced settings of the Access Point.
 - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.
 - **Management.** Modify UPnP, System Log, and SNMP settings.

3.1.2. Save, Save & Restart, and Cancel Commands

At the bottom of each page that contains settings you can configure, there are up to three buttons—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores the settings changes to the memory of the Access Point and brings you back to the **Summary** page. Clicking **Save & Restart** stores the settings changes to the memory of the Access Point and restarts the Access Point immediately for the settings changes to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.



Fig. 9. Save, Save & Restart, and Cancel.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in **red**. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the Access Point for the settings changes to take effect.

Fig. 10. Settings have been changed.

3.1.3. Home and Refresh Commands

At the bottom of a status page, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the **Summary** page. Clicking **Refresh** updates the shown status information.



Fig. 11. Home and Refresh buttons

3.2. Viewing Status

3.2.1. Associated Wireless Clients

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has sent, number of bytes it has received, and the time of its last activity, is shown.



Fig. 12. Status of associated wireless clients

3.2.2. Current DHCP Mappings

On this screen, all the current *static* or *dynamic* DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

DHCP Mapping Table			
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

Fig. 13. Current DHCP mappings

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page (see Section 3.4.2). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **Allocateable IP address count** settings on the **DHCP Server** configuration page.

3.2.3. System Log

System events are recorded in the memory of the Access Point. The logged information is useful for troubleshooting purposes. See Section 3.6.2.2 for more information.

Model:	AP Adv
BIOS/Firmware version:	APYS-8947 v1.4/1.5.3.3931
Operational mode:	Simple Access Point
Current time:	07/02/2003 15:05:56
07/02/2003 13:33:57 SYSTEM START UP!	
07/02/2003 13:33:57 Wireless LAN interface initializes success.	
07/02/2003 13:33:57 BSSID --> 00-90-4B-00-B9-BD	
07/02/2003 13:33:57 LAN IP address --> 192.168.168.214.	
07/02/2003 15:00:30 The administrator from 192.168.168.128 logs in the device successfully.	
07/02/2003 15:05:49 The administrator from 192.168.168.220 logs in the device successfully.	

Fig. 14. System log

3.2.4. Link Monitor

When the Access Point is in *AP Client* mode, use the Link Monitor feature to monitor the link quality and signal strength of the connection. Larger values mean better wireless connectivity to the Access Point.

Linking Quality :	10 %
Signal Strength :	25 %

Fig. 15. Link monitor

NOTE: The values are updated every 20 seconds.

3.3. General Operations

3.3.1. Specifying Operational Mode

- AP / Bridge**
This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- AP Client**
This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Fig. 16. Operational mode settings

The Access Point supports two operational modes:

- **AP/Bridge.** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- **AP Client.** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

In either mode, the Access Point forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 2 types of wireless links as specified by the IEEE 802.11 standard.

- **STA-AP.** This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The AP Client mode is actually an STA.
- **WDS.** This type of wireless link is established between two IEEE 802.11 Access Point's. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP/Bridge	AP Client
AP/Bridge	WDS	STA-AP
AP Client	STA-AP	

Table 2. Operational modes vs. wireless link types

To establish a *static* bridge link based on WDS, the AP/bridges at both end of the WDS link must be *manually* configured with each other's MAC addresses (see Section 3.5.1.5 for more information). To establish a *dynamic* bridge link between a Access Point and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any Access Point that is using the matched SSID and establishes a bridge link with the scanned Access Point.

NOTE: Although it's more convenient to use dynamic bridging, it has a limitation—the AP Client only can forward TCP/IP packets between its wireless interface and Ethernet interface; other type of traffic (such as IPX and AppleTalk) is not forwarded.

TIP: When the Access Point is configured to be in AP Client, it can be used as an Ethernet-to-wireless network adapter. For example, a notebook computer equipped with an Ethernet adapter can be connected to this device with a crossover Ethernet cable for wireless connectivity to another access point.

3.3.2. Changing Password

On this screen, the user name and password may be changed. The new password must be typed twice for confirmation.

Old password:	*****
New user name:	admin
New password:	*****
New password again:	*****

Fig. 17. Password

3.3.3. Managing Firmware

Firmware management operations for the Access Point include *firmware upgrade*, *configuration backup*, *configuration restore*, and *configuration reset*. Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP.



Fig. 18. Firmware management protocol setting

The HTTP method is suggested since it is more user friendly. However, due to different behavior of various Web browsers, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-method.

3.3.3.1. Upgrading Firmware by HTTP

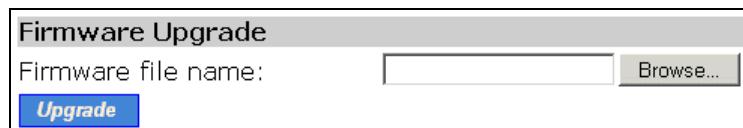


Fig. 19. Firmware upgrade by HTTP

To upgrade firmware of the Access Point by HTTP:

1. Click **Browse** and then select a correct firmware **.bin** file. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Upgrade** to begin the upgrade process.

3.3.3.2. Backing up and Restoring Configuration Settings by HTTP



Fig. 20. Firmware backup by HTTP

To back up configuration of the Access Point by HTTP:

1. Click **Back Up**.
2. You'll be prompted to open or save the configuration file. Click **Save**.
3. The configuration file is named by the Access Point's MAC address. For example, if the Access Point's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex". Don't change the configuration file name in the **Save As** dialog box. Select a folder in which the configuration file is to be stored. And then, click **Save**.

NOTE: The procedure may be a little different with different Web browsers.

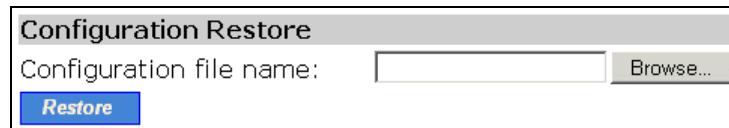


Fig. 21. Configuration restore by HTTP

To restore configuration of the Access Point by HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file name is the AP's MAC address. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Restore** to upload the configuration file to the Access Point

3.3.3.3. Upgrading Firmware by TFTP

To configure settings for the Access Point's TFTP client to communicate with a TFTP server, select TFTP as the firmware management protocol.

TFTP server IP address:	<input type="text" value="192.168.0.19"/>
Max number of retries:	<input type="text" value="30"/>
Timeout:	<input type="text" value="10 sec."/>

Fig. 22. TFTP server settings.

. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. The **Max number of retries** setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server.



Fig. 23. Firmware upgrade by TFTP

To upgrade firmware of the Access Point by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure IP address of the computer so that the Access Point and the computer are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP

address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the firmware upgrade process by clicking **Upgrade**.

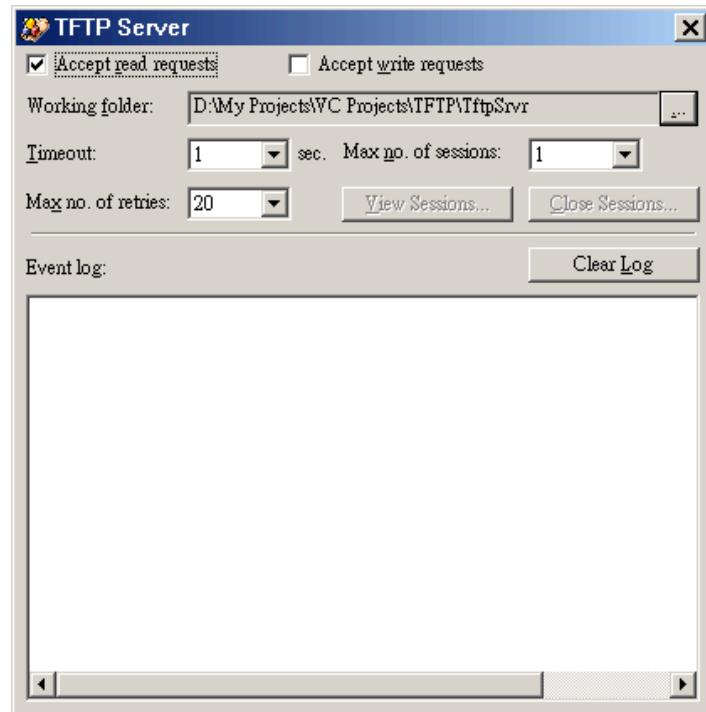


Fig. 24. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

NOTE: Make sure the **Accept read requests** check box of TFTP Server is selected.

NOTE: The LAN IP address of the Access Point and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless Access Point be connected by Ethernet, and on the same LAN, so that the upgrade process would be smooth.

NOTE: After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.

NOTE: A failed upgrade may corrupt the firmware and make the Access Point unbootable. When this occurs, call for technical support.

TIP: If you want to remotely upgrade the firmware of a deployed Access Point from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP upgrade to succeed.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP



Fig. 25. Configuration backup/restore

To back up configuration of the Access Point by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the Access Point are in the same IP subnet.
4. On the computer, run the TFTP Server utility. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the Access Point will be saved.
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type `IpConfig`, then press the **Enter** key.
8. Trigger the backup process by clicking **Back Up**. The Access Point's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "**AaBbCcDdEeFf**" is the AP's MAC address. For example, if the AP's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

NOTE: Remember to select the **Accept write requests** check box of TFTP Server.

To restore configuration of the Access Point by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the Access Point are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the configuration backup file resides. A configuration backup file is named by the AP's MAC address. For example, if the AP's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.

7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type **IpConfig**, then press the **Enter** key.
8. Trigger the restoring process by clicking **Restore**. The Access Point will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the Access Point.

TIP: If you want to remotely back up or restore configuration from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

3.3.3.5. Resetting Configuration to Factory Defaults

Clicking the **Reset** button resets the device configuration to factory defaults.

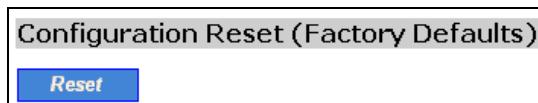


Fig. 26. Configuration reset

WARNING: Think twice before using the **Reset** button, as all your current configuration settings will be removed.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing

The IP address of the Access Point can be manually set (**Set Manually**) or automatically assigned by a DHCP server on the LAN (**Obtain from a DHCP Server**). If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the Access Point.

Method of obtaining an IP address:	<input type="button" value="Set Manually"/>
IP address:	192.168.168.214
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0
Host name:	AP1
Domain (DNS suffix):	

Fig. 27. TCP/IP settings

3.4.2. DHCP Server

3.4.2.1. Basic

The Access Point can automatically assign IP addresses to client computers by DHCP. From this screen, you can specify the **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of IP addresses available for allocation.

Functionality:	Disabled
Default gateway:	192.168.0.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.0.1
Secondary DNS server:	
First allocatable IP address:	192.168.0.2
Allocatable IP address count:	20

Fig. 28. Basic DHCP server settings.

NOTE: There should be only *one* DHCP server on the LAN; otherwise, DHCP would not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the Access Point.

NOTE: By default the DHCP server function is disabled.

3.4.2.2. Static DHCP Mappings

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. By **Static DHCP Mappings**, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP and it is always assigned the same IP address.

Enabled	Desc.	MAC Address	IP Address
<input type="checkbox"/>	Bill	00-22-32-5D-80-02	192.168.0.203
<input type="checkbox"/>			

Fig. 29. Static DHCP mappings

To always assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description for this mapping.
2. Select the corresponding **Enabled** check box.

3.5. Configuring IEEE 802.11 Related Settings

3.5.1. Communication

3.5.1.1. Basic

Basic IEEE 802.11g-related communication settings include **Access Point functionality**, **RF type**, **Regulatory domain**, **Channel number**, **Multiple Network name (SSID)**, **Data rate**, and **Transmit power**.

For specific needs such as configuring the Access Point as a wireless LAN-to-LAN bridge, the Access Point functionality can be disabled, so that no wireless client can associate with the Access Point.

AP functionality:	Enabled
RF type:	Mixed
Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	wireless
Data rate:	Auto
Transmit power:	High

Fig. 30. Basic IEEE 802.11g communication settings

The RF type of the WLAN interface can be configured to work in IEEE 802.11n only (**n Only**), IEEE 802.11g only (**g Only**), or mixed mode (**Mixed**—802.11n and 802.11g and 802.11b simultaneously).

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the Access Point must be identical for them to communicate with each other.

If there is RF interference, you may want to reduce the **Data rate** for more reliable wireless transmission. In most cases, leave the setting to **Auto**.

The transmit power of the RF module of the Access Point can be adjusted so that the RF coverage of the Access Point can be changed.

3.5.1.2. Link Integrity

Functionality:	<input type="button" value="Disabled"/>
Reference host:	<input type="text" value="0.0.0.0"/>

Fig. 31. Link integrity settings

When the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the Access Point and no wireless client can associate with the Access Point. The detection mechanism is based on pinging the IP address specified in **Reference host**.

3.5.1.3. Association Control

Max number of clients (1~64):	<input type="text" value="64"/>
Block clients if traffic load exceeds:	<input type="button" value="Disabled"/>

Fig. 32. Association control settings

If the number of currently associated wireless clients exceeds the value specified in the **Max number of clients** setting, no more wireless client can associate with the Access Point. If traffic load of the Access Point exceeds the load specified in the **Block clients if traffic load exceeds** setting, no more wireless client can associate with the Access Point.

3.5.1.4. Load Balancing

Several Access Point's can form a load-balancing group if they are set with the same **Group ID**. The load-balancing policy can be by **Number of Users** or by **Traffic Load**.

Functionality:	<input type="button" value="Enabled"/>
Group ID:	<input type="text" value="APLB_Group"/>
Policy by:	<input type="button" value="Number of Users"/>

Fig. 33. Access Point load balancing settings

If the *by-number-of-users* policy is selected, a new wireless user can only associate with an Access Point that has the smallest number of associated wireless users in the group. On the other hand, if the *by-traffic-load* policy is selected, a new wireless user can only associate with an Access Point that has the less traffic load in the group.

3.5.1.5. Wireless Distribution System

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 34, AP 2 acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 plays a role of “AP repeater”.

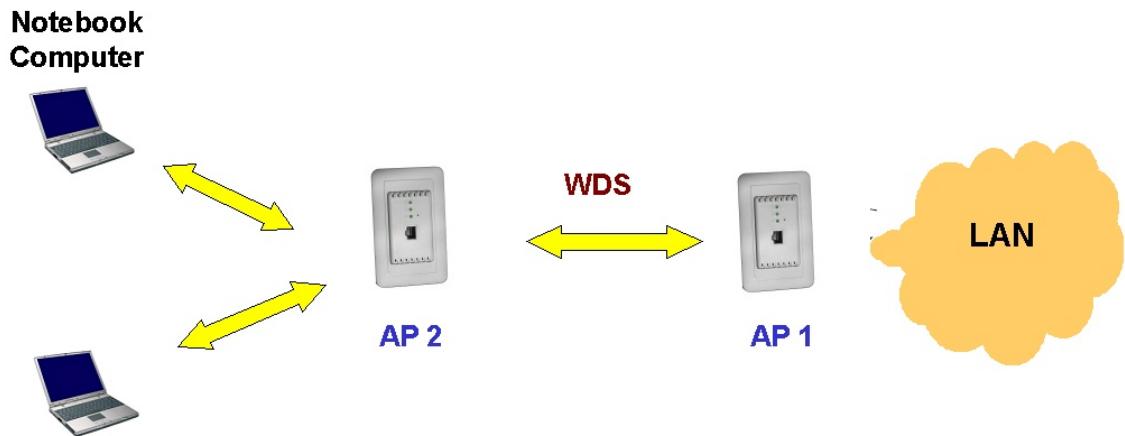


Fig. 34. Wireless Distribution System

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 35, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the Access Point is WDS-enabled, it can be used as a wireless bridge.



Fig. 35. LAN-to-LAN bridging

NOTE: A Access Point can have up to 6 WDS links to other APs or wireless bridges.

Port Enabled	Peer MAC Address
1 <input type="checkbox"/>	00-02-6F-01-62-C5
2 <input type="checkbox"/>	
3 <input type="checkbox"/>	
4 <input type="checkbox"/>	
5 <input type="checkbox"/>	
6 <input type="checkbox"/>	

Fig. 36. Wireless Distribution System settings

To enable a WDS link:

1. Specify the MAC address of the Access Point at the other end of the WDS link.

2. Select the corresponding **Enabled** check box.

For example, assume you want two Access Point's with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On Access Point 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AP 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP: Plan your wireless network and draw a diagram, so that you know how a Access Point is connected to other peer Access Point s or wireless bridges by WDS.

TIP: Plan your wireless network and draw a diagram, so that you know how a bridge is connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.

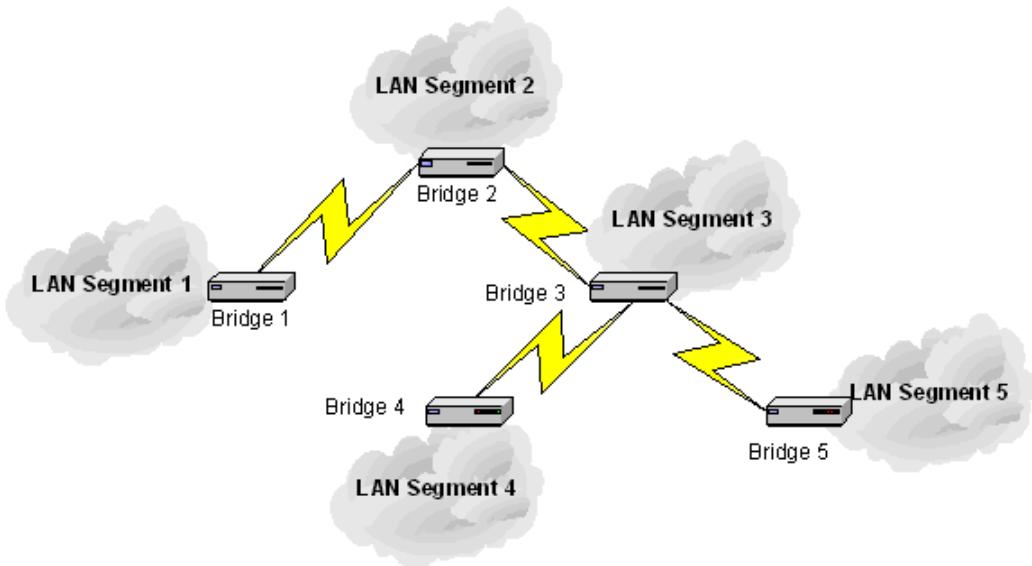


Fig. 37. Sample wireless bridge network topology.

WARNING: Don't let your network topology consisting of wireless bridges, Ethernet switches, Ethernet links, and WDS links contain *loops*. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.

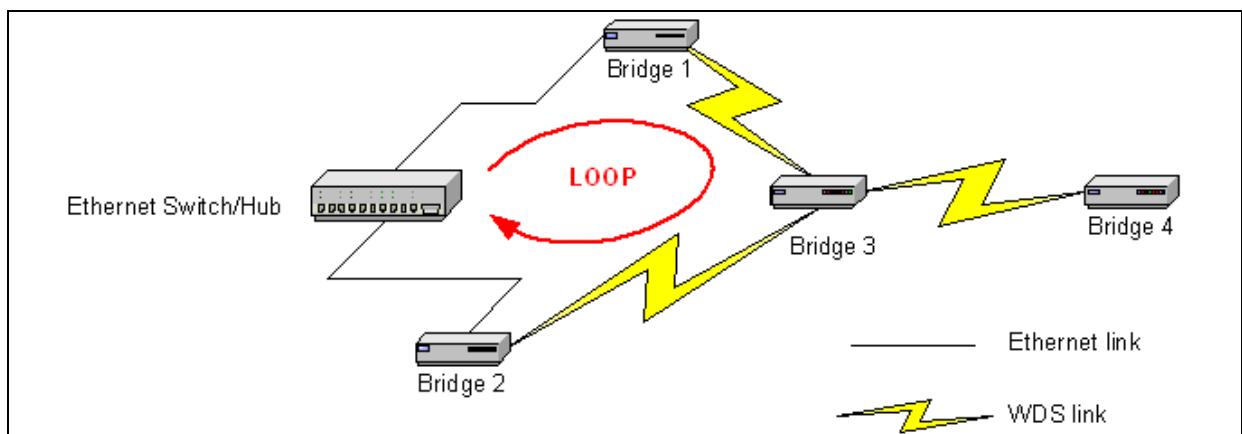
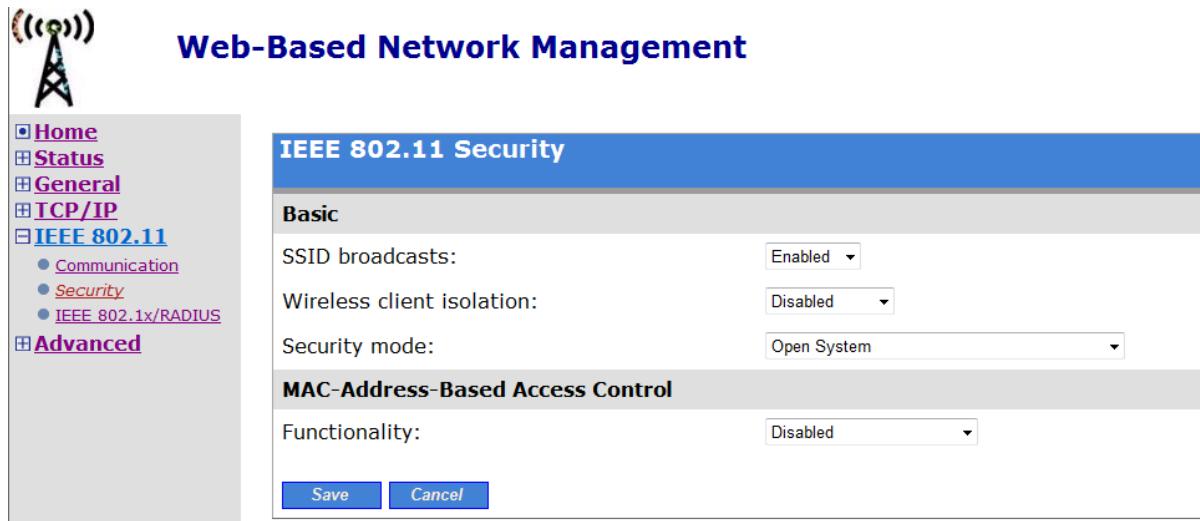


Fig. 38. Network topology containing a loop

If external high-gain *directional* antennas are used, it's difficult to align the antennas when the distance between the bridges is long.

3.5.2. Security

IEEE 802.11g security settings include **SSID broadcasts**, **Wireless client isolation**, **Security mode**, , **MAC-Address-Based Access Control**.



The screenshot shows a web-based network management interface. The left sidebar has a tree view with nodes: Home, Status, General, TCP/IP, IEEE 802.11 (selected), and Advanced. The IEEE 802.11 node has sub-nodes: Communication, Security, and IEEE 802.1x/RADIUS. The main content area is titled "IEEE 802.11 Security". It has two sections: "Basic" and "MAC-Address-Based Access Control". In the "Basic" section, "SSID broadcasts" is set to "Enabled", "Wireless client isolation" is set to "Disabled", and "Security mode" is set to "Open System". In the "MAC-Address-Based Access Control" section, "Functionality" is set to "Disabled". At the bottom are "Save" and "Cancel" buttons.

TABLE OF SECURITY SETTING DEFINITIONS

SSID	The network name
SSID Broadcasts	Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network.
Wireless Client Isolation	When the Access Point is in AP/Bridge mode, wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users' computers.
Security mode	The Security options for the primary SSID (SSID1) are up to 9 security modes depending on AP model variations:

Open System. No authentication, no data encryption.

Static WEP
802.1x with Dynamic WEP (EAP-TLS,PEAP)
WPA-PSK with TKIP
WPA-PSK with AES
WPA2-PSK with TKIP
WPA2-PSK with AES
WPA with TKIP
WPA with AES
WPA2 with TKIP
WPA2 with AES

3.5.2.1. Selecting Wireless Security Mode

For security reasons, it's highly recommended that the security mode be set to options other than *Open System*. When the security mode is set to Open System, no authentication and data encryption will be performed. Additionally, you can *disable* the SSID broadcasts functionality so that a wireless client computer with an “any” SSID cannot associate with the AP.

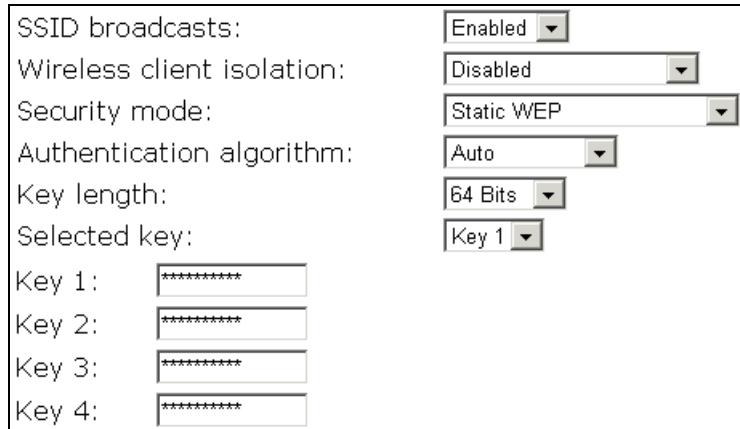


Fig. 38. Basic IEEE 802.11g security settings

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients of this Access Point cannot see each other, and wireless-to-wireless traffic is blocked. This feature is useful for WLANs deployed in public places. In this way, hackers have no chance to attack other wireless users in a *hotspot*.

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients (STAs) of this Access Point cannot see each other, and wireless-to-wireless traffic between the STAs is blocked.

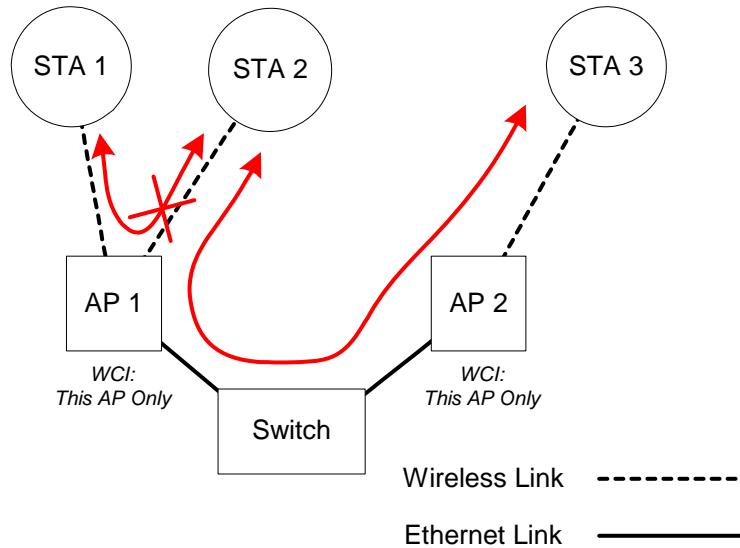


Fig. 39. Behavior of the “This AP Only” wireless client isolation option

As illustrated in Fig. 39 when AP 1 and AP 2 are using the “This AP Only” option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3,

which are associated with different APs, is still allowed.

Choose from up to 7 security modes:

- **Open System.** No authentication, no data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.
- **Static TKIP (WPA-PSK).** Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the **Pre-shared key**, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

NOTE: The **Pre-Shared Key** has a minimum of 8 and maximum of 63 characters.

- **IEEE 802.1x EAP without Encryption (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.
- **IEEE 802.1x EAP with Static WEP (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.
- **IEEE 802.1x EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP).** The IEEE 802.1x functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.
- **IEEE 802.1x EAP with Dynamic TKIP (WPA).** This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The Access Point is highly secured in this mode.

In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled. See Section 3.5.3 for more information about IEEE 802.1x and RADIUS.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, *Shared Key* authentication is used if WEP data encryption is enabled. In rare cases, *Open System* authentication may be used when WEP data encryption is enabled. The **Authentication algorithm** setting is provided for better compatibility with wireless clients with various WLAN network adapters. There are three options available, including *Open System*, *Shared Key*, and *Auto*.

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the Access Point side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the Access Point side.

NOTE: Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to “00012E3ADF”.

3.5.2.2. MAC-Address-Based Access Control

When the **MAC-Address-Based Access Control** feature, the wireless client computers that are permitted or not permitted to associate with the Access Point can be specified. When the table type is set to *inclusive*, entries in the table are permitted to associate with the Access Point. When the table type is

set to *exclusive*, entries in the table are not permitted to associate with the Access Point.

Functionality:	<input type="button" value="Enabled"/>
Access control type:	<input checked="" type="radio"/> inclusive <input type="radio"/> exclusive
<input type="button" value="Add"/>	
MAC address format: 00-02-DD-30-03-1E	
MAC Address	Delete
00-50-C2-01-96-4D	<input type="button" value="Delete"/>
00-09-92-01-02-55	<input type="button" value="Delete"/>

Fig. 40. MAC-address-based access control settings

To deny wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *exclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To grant wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *inclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To delete an entry in the access control table:

- Click **Delete** next to the entry.

NOTE: The size of the access control table is 64.

TFTP server IP address:	<input type="text" value="192.168.0.125"/>
MAC ACL file name:	<input type="text" value="MacAcl.txt"/>
<input type="button" value="Download"/>	

Fig. 41. MAC ACL download settings

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the Access Point to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 42 shows the contents of a sample ACL file.

00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
00-11-22-33-44-60

Fig. 42. Sample MAC ACL file

To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.
2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.
3. Click **Download**.

3.5.3. IEEE 802.1x/RADIUS

IEEE 802.1x *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the access point is controlled by the *security mode* (see Section 錯誤! 找不到參照來源。). So far, the wireless access point supports two authentication mechanisms—EAP-MD5 (Message Digest version 5), EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user has to give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access point. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

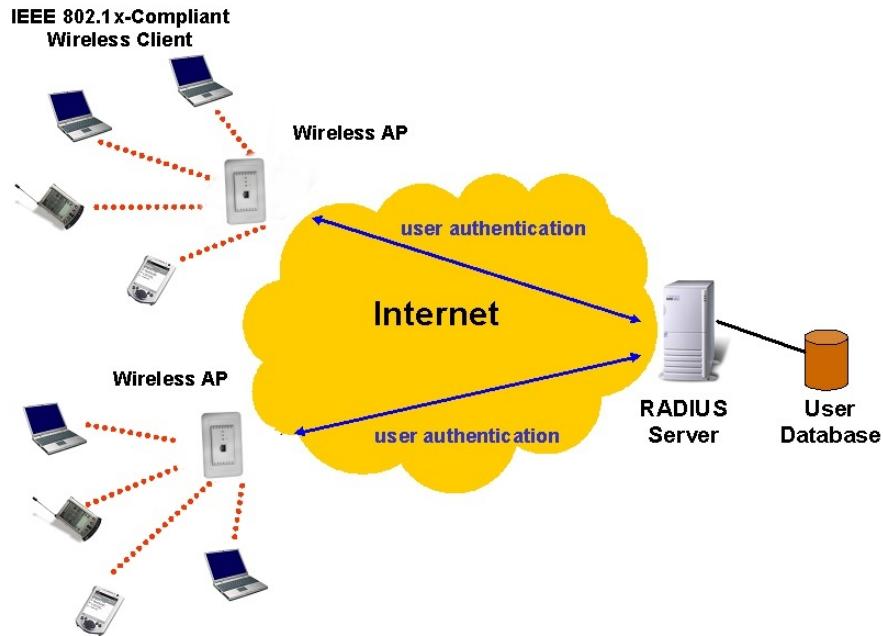


Fig. 43. How IEEE 802.1x and RADIUS works

An access point supporting IEEE 802.1x can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the wireless access point will try to communicate with the secondary RADIUS server. You can specify the length of timeout and the number of retries before communicating with the *secondary* RADIUS server after failing to communicate with the primary RADIUS server.

An IEEE 802.1x-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a wireless access point can identify itself by an NAS (Network Access Server) identifier. Each IEEE 802.1x-capable wireless access point must have a *unique* NAS identifier.

Primary RADIUS server:	<input type="text" value="192.168.168.220"/>
Secondary RADIUS server:	<input type="text"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Timeout (sec.):	<input type="text" value="5"/>
Max number of retries:	<input type="text" value="3"/>
Shared key:	<input type="text" value="*****"/>
Identifier of this NAS:	<input type="text" value="AP1"/>

Fig. 44. IEEE 802.1x/RADIUS settings.

TIP: Refer to the IEEE 802.1x-related white papers on the companion CD-ROM for more information about deploying secure WLANs with IEEE 802.1x support.

3.6. Advanced Settings

3.6.1. Packet Filters

The Access Point Web-Based Network Management provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

Functionality: Sets the filtering as *enabled* or *disabled*.

Policy for matched packets: Choose to *discard* or to *pass* a matched packet.

To enable a filtering rule: Select the check box to the left of the rule to enable.

3.6.1.1. Ethernet Type Filters

When this feature is enabled, the *Ethernet type* field of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. To set a rule, specify the hex-decimal Ethernet type number and give the rule a name.

Functionality:	Disabled
Policy for matched packets:	Discard
Name	Number
<input checked="" type="checkbox"/> RARP	0x8035
<input type="checkbox"/> ARP	0x0806
<input type="checkbox"/> NetBUI	0xF0F0
<input type="checkbox"/> Novell IPX	0x8138
<input type="checkbox"/> IPX 802.3	0x00FF

Fig. 45. Ethernet type filters settings

3.6.1.2. IP Protocol Filters

When this feature is enabled, the protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. To set a rule, specify the hex-decimal protocol number, source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

Functionality:	Disabled			
Policy for matched packets:	Discard			
Protocol Number	Source Address	Subnet Mask	Destination Address	Subnet Mask
<input checked="" type="checkbox"/> 0x01	192.168.0.3	255.255.255.255	192.168.0.5	255.255.255.255
<input type="checkbox"/> 0x02	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/> 0x06	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/> 0x11	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/> 0x62	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Fig. 46. IP protocol filters settings

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

3.6.1.3. TCP/UDP Port Filters

The *destination port* field the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering.

Functionality:	Disabled	
Policy for matched packets:	Discard	
Destination Port	Protocol	Application Name
<input checked="" type="checkbox"/> 80	TCP	HTTP
<input type="checkbox"/> 0	TCP	

Fig. 47. TCP/UDP port filters settings

To set a rule, specify the decimal **Destination Port**, **Protocol** type (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

3.6.2. Management

3.6.2.1. UPnP

The UPnP (Universal Plug and Play) features enables a Windows XP user to automatically discover peripheral devices by HTTP.

Functionality:	Enabled
Device friendly name:	Wireless AP

Fig. 48. UPnP settings

When the UPnP functionality is enabled, you can see the Access Point in My Network Places of Windows XP. The Access Point can be given a *friendly name* that will be shown in My Network Places. *Double-clicking* the Access Point icon in My Network Places will launch the default Web browser for you to configure the AP.

3.6.2.2. System Log

System events can be logged to the on-board RAM of the Access Point (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

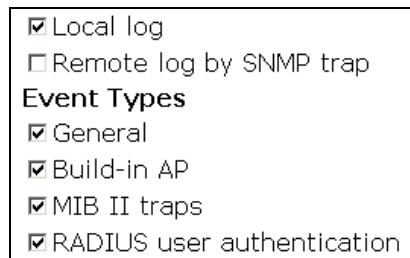


Fig. 49. System log settings

The system events are divided into the following categories:

- **General:** System and network connectivity status changes.
- **Built-in AP:** Wireless client association and WEP authentication status changes.
- **MIB II traps:** *Cold Start*, *Warm Start*, *Link Up*, *Link Down* and *SNMP Authentication Failure*.
- **RADIUS user authentication:** RADIUS user authentication status changes.

NOTE: The *SNMP Authentication Failure* trap is issued when using an incorrect community string to manage the Access Point via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

3.6.2.3. SNMP

The SNMP (Simple Network Management Protocol) functionality can be disabled, and you can specify the name (used as a *password*) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap Table**.

Functionality:	Enabled <input type="button" value=""/>
Read-only community:	*****
Read-write community:	*****
SNMP Trap Table	
IP Address	Community
<input checked="" type="checkbox"/> 192.168.0.2	*****
<input type="checkbox"/> 0.0.0.0	

Fig. 50. SNMP settings

To specify a trap target:

1. Type the IP address of the target host.
2. Type the **Community** for the host.
3. Select the corresponding check box next to the IP address text box.

Appendix A: Default Settings

TIP: Press the **Default (SF-Reset, or Soft-Reset)** switch on the housing of a *powered-on* Access Point to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
IEEE 802.11g	
Regulatory Domain	FCC (U.S.)
Channel Number	1
SSID	Wireless
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the accompanying PCMCIA card or the label on the housing of the AP.
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
AP Load balancing	Disabled
Link Integrity	Disabled
Association Control	
Max Number of Clients	64
Block Clients if Traffic Load Exceeds	Disabled
LAN Interface	
Method of obtaining an IP Address	Obtain from a DHCP Server
IP Address	192.168.100.1 (if can't get IP)
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
DHCP Server	Disabled
Management	
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private

Appendix B: Troubleshooting

Check the following first:

- Verify that Access Point is powered-on and any Ethernet cables are connected firmly to the RJ-45 jacks of the Access Point.
- Verify that the LED ALV of the Access Point is blinking to indicate the Access Point is working.
- Check that the types of Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.

B-1: Wireless Settings Problems

- **The wireless client computer cannot associate with the Access Point.**
 - Is the wireless client in *infrastructure* mode?
 - ◆ Check the *operating mode* of the wireless adapter.
 - Is the SSID identical to that of the Access Point?
 - ◆ Verify that the SSID setting of the wireless adapter matches that of the Access Point.
 - Is the WEP enabled?
 - ◆ If necessary, ensure that the appropriate WEP settings of the client computer match the Access Point.
 - Is the Access Point within range of wireless communication?
 - ◆ Check the *signal strength* and *link quality* sensed by the wireless adapter.

B-2: TCP/IP Settings Problems

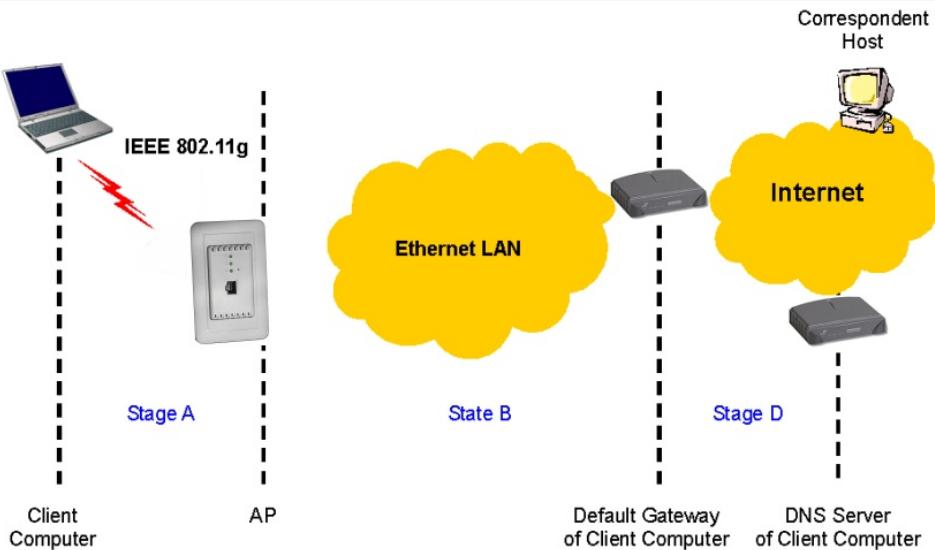


Fig. 51. Communication stages for a client to reach its correspondent host

For a wireless client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. <http://www.wi-fi.com>), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the AP, then the Access Point relays this request to the default gateway of the client computer. Finally, this request is forwarded by the gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP address.

As illustrated in Fig. 51, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, **ping.exe**, can be employed to find out TCP/IP-related communication problems.

NOTE: If *two or more* NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, **route.exe**, to add or delete entries from the routing table. Or, use Windows-provided **Device Manager** to disable unnecessary NICs.

Solve the following problems in order:

- **The Access Point does not respond to *ping* from the client computer.**
 - Are two or more NICs installed on the client computer?
 - ◆ Use the OS-provided command-line network tool, **route.exe**, to modify the contents of the routing table.
 - ◆ Use Windows-provided **Device Manager** to disable unnecessary NICs.
 - Is the underlying link (Ethernet or IEEE 802.11g) established?
 - ◆ Make sure the Ethernet link is OK.
 - ◆ Make sure the wireless settings of the wireless client computer and of the Access

Point match.

- Are the IP address of the *client computer* and the IP address of the *Access Point* in the same IP subnet?
 - ◆ Use **WinIPCfg.exe** or **IPConfig.exe** to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the Access Point are in the same IP subnet.
 - ◆ **TIP:** If you forget the current IP address of the AP, use Wireless Router/AP Browser to get the information (see Appendix B-3).
- **The default gateway of the client computer does not respond to *ping* from the client computer.**
 - Solve the preceding problem first.
 - Are the IP address of the *Access Point* and the IP address of the *client computer* in the same IP subnet?
 - If you cannot find any incorrect settings of the AP, the default gateway may be really down or there are other communication problems on the network backbone.
- **The DNS server(s) of the client computer do not respond to *ping* from the client computer.**
 - Solve the preceding problems first.
 - If you cannot find any incorrect settings of the AP, the default gateway of the Access Point may be really down or there are other communication problems on the network backbone.